UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/521,788	03/09/2000	Michael S. Borella	99,720	3011

20306 7590 02/10/2004

MCDONNELL BOEHNEN HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
SUITE 3200
CHICAGO, IL 60606

EXAMINER	
ZIA, MOSSADEQ	

ART UNIT	PAPER NUMBER
2134	6

DATE MAILED: 02/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/521,788	BORELLA ET AL.	
	Examiner	Art Unit	
	Mossadeq Zia	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3,4,5*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As seen on page 40, claim 4, the applicant refers to same claim for dependence. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claim 1-3, 5, 6-15, 18, 19, 21, 23, 24, 25, 27 are rejected under 35 U.S.C. 102(b) as anticipated by "IPv6: The New Internet Protocol", Christian Huitema.

5. Regarding claim 1, Huitema discloses a computer network with a plurality of network devices, a method for distributed generation of unique random numbers for digital cookies, comprising the steps of:

generating a first portion of a x-bit digital cookie (half-key) on a first network device (initiator) on the computer network based on an x-bit bit mask template (number space chosen by

responder) sent to the first network device from a second network device on the computer network (responder, Huitema, page 109, 3rd paragraph);

sending a first message to request a second portion of the x-bit digital cookie (key request) from the second network device, wherein the first message includes the first portion of the x-bit digital cookie (Huitema, page 109, 4th paragraph, line 1-4);

receiving a first response from the second network device wherein the first response includes a second portion of the x-bit digital cookie from the second network device (Huitema, page 109, 5th paragraph, line 4-5, page 110, 1st paragraph, line 1-2), and wherein the second network device generates potential x-bit digital cookies using the first portion of the x-bit digital cookie from the first network device and a second portion of the x-bit digital cookie generated on the second network device (session keys,Huitema, page 110, 2nd paragraph, line 2-5, 2nd table) until the second network device generates a potential x-bit digital cookie that is not in use on the computer network (page 111, 3rd paragraph, line 2-4);

generating a complete x-bit digital cookie on the first network device using the first portion of the x-bit digital cookie and the second portion of the x-bit digital cookie, wherein the complete x-bit digital cookie is not in use on the computer network (Huitema, page 111, 1st paragraph, line 2).

6. Regarding claims 2, 11, 18, 24, Huitema discloses claim 1 above, and further discloses a computer readable medium having stored therein instructions for causing a central processing unit to execute the method (Huitema, computed, page 110, 2nd paragraph, line 3, page 119, paragraph 4, line 2-3).

7. Regarding claims 3, 21, Huitema discloses claim 1 above, and further disclose: sending the complete x-bit digital cookie in a plurality of messages used to a establish a secure connection between the first network device on the computer network and third network device on a remote computer network (Huitema, page 113, 3rd paragraph, line 5-6, page 115, 5th paragraph, line 1-3).

8. Regarding claims 5, 12, Huitema discloses claim 1 above, and further discloses the step of generating a first portion of an x-bit digital cookie includes generating a n-bit random number, wherein the number-n is determined by counting n-number of bits set to a value of one in the x-bit bit mask sent to the first network device by the second network device (number space, page 106, 4th paragraph, page 107, 1st paragraph).

9. Regarding claims 6, 13, Huitema discloses claim 1 above, and further disclose the second portion of the bit mask is an (x-n) bit random number generated on the second network device, wherein n is less than or equal to x (vector length, Huitema, page 108, 2nd paragraph, line 6-7).

10. Regarding claims 7, 15, 19, 25, Huitema discloses claim 1 above, and further disclose the x-bit bit mask template is a 64-bit, bit mask template (Huitema, page 108, 2nd paragraph, line 7).

11. Regarding claims 8, 14, 27, Huitema discloses claim 1 above, and further disclose the step of generating a complete x-bit digital cookie on the first network device includes generating a complete x-bit digital cookie on the first network device by placing values of bits from the first portion of the x-bit digital cookie in bit positions with a value of one using the x-bit bit mask template, and by placing values of bits from the second portion of the x-bit digital cookie in bit positions with a value of zero using the x-bit bit mask template (Huitema, page 110, 2nd table, line 7).

12. Regarding claims 10 and 23, Huitema discloses a computer network with a plurality of network devices, a method for distributed generation of unique random numbers for digital cookies, comprising the steps of:

maintaining a list of complete digital cookies in use on the computer network on a second network device (Huitema, computed, page 111, 2nd paragraph, line 5-6);

generating a x-bit bit mask template on a second network device, wherein the x-bit bit mask has n-bits randomly set to a value of one and remaining (x-n) bits randomly set to value of zero wherein n is less than or equal to x (number space, page 106, 4th paragraph, page 107, 1st paragraph, page 108, 1st paragraph, line 2-3, Table- value of 0 defines padding);

sending the x-bit bit mask template to a first network device on the computer network (responder, Huitema, page 109, 3rd paragraph);

receiving a request from the first network device to request a second portion of a x-bit digital cookie from the second network device, wherein the first message includes an first portion of the x-bit digital cookie (responder, Huitema, page 109, 4th paragraph);

(a) generating a second portion of a x-bit digital cookie on the second network device (Huitema, page 110, 2nd paragraph, line 2-5);

(b) generating a potential x-bit digital cookie on the second network device using the first portion of the x-bit digital cookie generated on the first network device and the second portion of the x-bit digital cookie generated on the second network device (Huitema, page 111, 1st paragraph, line 2);

(c) comparing the potential x-bit digital cookie with complete digital cookies from the list of complete digital cookies maintained on the second network device that are in use on the computer network (page 111, 2nd paragraph, line 5-7);

repeating steps (a), (b), and (c) until a potential x-bit digital cookie is generated that is not in use on the computer network; and sending the second portion of the x-bit digital cookie for the potential x-bit digital cookie that is not in use on the computer network to the first network device, wherein the first network device uses the first portion of the x-bit digital cookie and the second portion of the x-bit digital cookie to create a complete x-bit digital cookie that is not in use on the computer network (page 111, 3rd paragraph, line 2-4).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 4, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over "IPv6: The New Internet Protocol", Christian Huitema in view of "The Internet Key Exchange (IKE)" by Harkins et al.

13. Regarding claims 4, 22, Huitema discloses claim 1 above, but fail to disclose the plurality of messages include a plurality of Internet Key Exchange protocol messages.

However, Harkins et al. teach that attributes are used by IKE and are negotiated as part of the Internet Security Association and Key Management Protocol (ISAKMP) Security Association (Harkins, page 6, 5th paragraph) where ISAKMP is designed to be key exchange

independent; that is, it is designed to support many different key exchanges (Harkins, page 2, Abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Huitema as per teaching of Harkins to include IKE to gain the benefit of framework for authentication and key exchange (Harkins, page 2, Abstract).

14. Claims 9, 16, 20, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over "IPv6: The New Internet Protocol", Christian Huitema in view of "RSIP Support for End-to-end IPSEC" by Montenegro et al.

15. Regarding claims 9, 16, 20, 26, Huitema discloses claim 1 above, but fails to disclose the second network device is any of a Distributed Network Address Translation gateway or a Realm Specific Internet Protocol gateway.

However, Montenegro teaches RSIP Protocol Extentions to enable end-to-end IPSEC where document proposes RSIP extensions and mechanisms to enable an RSIP client X to initiate IKE and IPSEC sessions to a legacy IKE and IPSEC node Y. In order to do so, X exchanges RSIP protocol messages with the RSIP server N (second network device, page 2, last paragraph and continuing one to page 3).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Huitema as per teaching of Montenegro to include RSIP gateway to gain the benefit of enabling end-to-end IPSEC sessions between RSIP client X and a legacy IKE and IPSEC node Y (page 2, Model diagram, 4th paragraph under section 2, and continuing one to page 3).

Conclusion

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is 703-305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-3900.

Mossadeq Zia
Examiner
Art Unit 2134

mz
1/21/04

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2